PCT

WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 :		(11) Internationale Veröffentlichungsnummer: WO 99/35781
H04L 9/00	A2	(43) Internationales Veröffentlichungsdatum: 15. Juli 1999 (15.07.99)

(21) Internationales Aktenzeichen: PCT/EP98/07984

(22) Internationales Anmeldedatum: 9. Dezember 1998 (09.12.98)

(30) Prioritätsdaten:
198 01 241.1 12. Januar 1998 (12.01.98) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: DEUTSCHE TELEKOM AG [DE/DE]; Friedrich-Ebert-Allee 140, D-53113 Bonn (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: MERTES, Paul [DE/DE]; Mertenseifer Grund 9, D-57258 Freudenberg (DE). METTKEN, Werner [DE/DE]; Eichenweg 9, D-59969 Hallenberg (DE).

(74) Gemeinsamer Vertreter: DEUTSCHE TELEKOM AG; Technologiezentrum, EK03, D-64307 Darmstadt (DE).

(81) Bestimmungsstaaten: CA, JP, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht
Ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts.

(54) Title: METHOD FOR GENERATING ASYMMETRICAL CRYPTOGRAPHIC KEYS BY THE USER

(54) Bezeichnung: VERFAHREN ZUR GENERIERUNG ASYMMETRISCHER KRYPTOSCHLÜSSEL BEIM ANWENDER

(57) Abstract

Users need signature and coding keys for generating asymmetrical cryptographic keys. Reliable connections to a trust center are required for personalization and certification. Security problems arise when users wish to generate their own keys, more particularly, cryptographic keys. Said problems are diminished by a method, wherein the user initially receives a generated, personalized and certified pair of keys and components for generating coding pairs from the trust center. At a given moment, the user produces a coding pair of keys, signs the public part of said pair with the secret signature key assigned to him or her and transmits the result to the trust center, where the result is assigned to the user by means of the certified public part of the signature pair of keys. The invention can be particularly applied in all forms of asymmetric cryptographic methods, basically in money cards and bank transactions, access controls to networks and data banks, admission controls to buildings or rooms, digital signatures, digital identification and patient cards.

(57) Zusammenfassung

Bei der Generierung asymmetrischer Kryptoschlüssel in Anwenderhand sind Signatur- und Verschlüsselungsschlüssel und bei der Personalisierung und Zertifizierung zuverlässige Verbindungen zu einem Trust Center erforderlich. Wenn Anwender eigene Schlüssel, insbesondere Kryptoschlüssel, generieren wollen, entstehen Sicherheitsprobleme. Derartige Probleme mindert ein Verfahren, bei dem der Anwender zunächst vom Trust Center ein generiertes, personalisiertes und zertifiziertes Schlüsselpaar sowie Komponenten zur Erzeugung von Verschlüsselungspaaren erhält. Der Anwender erzeugt irgendwann selbst ein Verschlüsselungsschlüsselpaar, signiert den öffentlichen Teil dieses Paares mit dem ihm überlassenen geheimen Signaturschlüssel und übermittelt das Ergebnis zum Trust Center, wo das Ergebnis mittels des zertifizierten öffentlichen Teils des Signaturschlüsselpaares dem Anwender zugeordnet wird. Anwendungsgebiet der Erfindung sind alle Formen asymmetrischer Kryptoverfahren: im wesentlichen Geldkarten/Banktransaktionen, Zugangskontrolle zu Netzwerken/Datenbanken, Zutrittskontrolle zu Gebäuden/Räumen, Digitale Signature, Digitale Ausweise/Patientenkarten.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidschan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland			TR	Türkei
BG	Bulgarien	HU	Ungarn	ML	Mali	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MN	Mongolei	UA	Ukraine
BR	Brasilien	IL	Israel	MR	Mauretanien	UG	Uganda
BY	Belarus	IS	Island	MW	Malawi	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	MX	Mexiko		
CF	Zentralafrikanische Republik	JP	Japan	NE	Niger	UZ	Usbekistan
CG	Kongo	KE	Kenia	NL	Niederlande	VN	Vietnam
CH	Schweiz	KG	Kirgisistan	NO	Norwegen	YU	Jugoslawien
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	NZ	Neuseeland	ZW	Zimbabwe
CM	Kamerun			PL	Polen		
CN	China	KR	Republik Korea	PT	Portugal		
CU	Kuba	KZ	Kasachstan	RO	Rumänien		
CZ	Tschechische Republik	LC	St. Lucia	RU	Russische Föderation		
DE	Deutschland	LI	Liechtenstein	SD	Sudan		
DK	Dänemark	LK	Sri Lanka	SE	Schweden		
EE	Estland	LR	Liberia	SG	Singapur		

Verfahren zur Generierung asymmetrischer Kryptoschlüssel beim Anwender

Beschreibung:

Die Erfindung bezieht sich auf ein asymmetrisches Kryptoverfahren der im Oberbegriff des Patentanspruchs 1 näher bezeichneten Art. Derartige Verfahren sind vielfach bekannt und z. B. in Menezes: Handbook of applied cryptography 1997 beschrieben.

Ein Kernproblem aller bekannten offenen Kryptoverfahren ist die zuverlässige Zuordnung der eingesetzten Signatur- und Verschlüsselungsschlüssel zum berechtigten Inhaber und die Bestätigung der Zuordnung durch eine unabhängige dritte Instanz. Fachsprachlich ist dies die Frage einer zuverlässigen Personalisierung der Schlüssel mit anschließender Zertifizierung.

Vertrauenswürdige Verfahren, wie z. B. von Kowalski, in Der Fernmeldeingenieur 4/5 1995,: „Security Management System" beschrieben, lösen dies heute, indem solche Schlüssel an zentraler, besonders abgesicherter Stelle (meist sogenannte Trust Center) generiert, personalisiert und zertifiziert werden.

Es ist jedoch nicht auszuschließen, daß die Anwender ihre Kryptoschlüssel, insbesondere jene zur Verschlüsselung, zukünftig zunehmend selbst generieren wollen. Dieser Wunsch darf dabei nicht auf Kosten der Sicherheit und Zuverlässigkeit des jeweiligen Verfahrens realisiert werden, wie dies heute bei nur lose organisierten asymmetrischen Kryptoverfahren des Internet der Fall ist.

Als Aufgabe der Erfindung bedarf es somit eines Verfahrens, welches die Schlüsselgenerierung in den Verantwortungsbereich der Anwender verlagert, ohne auf die organisatorische Sicherheit einer unabhängigen Instanz zu verzichten.

Diese Aufgabe wird mit dem im Kennzeichen des Patentanspruchs 1 aufgeführten Verfahren gelöst.

Vorteilhafte Weiterbildungsmöglichkeiten sind aus dem Kennzeichen des Unteranspruchs 2 ersichtlich.

Die Erfindung wird anhand des nachfolgenden Ausführungsbeispiels näher erläutert:

Der Anwender erhält von zentraler Stelle, nachfolgend allgemein als Trust Center bezeichnet, ein bereits generiertes personalisiertes und zertifiziertes Signaturschlüsselpaar, z. B. ein privater Signaturschlüssel PS und ein öffentlicher Signaturschlüssel ÖS sowie die Komponenten zur Erzeugung eines oder mehrerer Verschlüsselungsschlüsselpaare Generate Encryption Keys GEK.

Der Anwender erzeugt nun irgendwann selbst ein Verschlüsselungsschlüsselpaar, z. B. einen privaten Verschlüsselungsschlüssel PVS, signiert den öffentlichen Teil dieses Paares, den öffentlichen Verschlüsselungsschlüssel ÖVS mit dem zuvor überlassenen geheimen Signaturschlüssel PS, und übermittelt das Ergebnis an das Trust Center. Dort ist das Ergebnis über eine Prüfung mit Hilfe des zertifizierten öffentlichen Teiles des Signaturschlüsselpaares des Anwenders ÖS zweifelsfrei und zuverlässig als dem Anwender gehörend zuzuordnen.

Das Trust Center erzeugt daraufhin ein neues Zertifikat, in dem entweder sowohl der öffentliche Teil des Signaturschlüsselpaares ÖS als auch der des Verschlüsselungsschlüsselpaares ÖVS, oder nur der des Verschschlüsselungsschlüsselpaares des Anwenders ÖVS enthalten sind.

Dieses Zertifikat wird im nächsten Schritt mit dem öffentlichen Teil des Verschlüsselungsschlüsselpaares des Anwenders ÖVS verschlüsselt und dann übermittelt.

Damit ist sichergestellt, daß nur der berechtigte Anwender das Zertifikat entschlüsseln und, bei hardwarebasierten Systemen, in seine korrespondierende Hardware herunterladen kann. Der Anwender mußte zu keinem Zeitpunkt sein Geheimnis, nämlich den geheimen Teil des Verschlüsselungsschlüsselpaares PVS preisgeben.

Will der Anwender zusätzlich auch noch das Signaturschlüsselpaar in seinem Verantwortungsbereich erzeugen, also auch den geheimen Teil eines Signaturschlüsselpaares, einen zweiten privaten Signaturschlüssel PS2, vor dem Zugriff des Trust Center schützen, so wird dieses Verfahren auch dafür analog eingesetzt. Dem Anwender werden nur noch zusätzlich die Komponenten Generate Digital Signature Keys GDSK zur Erzeugung eines oder mehrerer Signaturschlüsselpaare überlassen.

Einmal erzeugt, signiert der Anwender, unter Zuhilfenahme des vom Trust Center überlassenen geheimen Signaturschlüssels PS, neben oder zugleich mit dem öffentlichen Teil des selbst generierten Verschlüsselungspaares ÖVS, auch noch den öffentlichen Teil des selbst generierten Signaturschlüsselpaares ÖS2 und übermittelt das Ergebnis an das

Trust Center, wo danach ebenso wie oben beschrieben, weiter verfahren wird.

Soweit der Anwender AW1 überhaupt keine Kommunikation mehr mit einem Trust Center wünscht, kann er auch dies mit dem beschriebenen Verfahren ohne Verlust an Zuverlässigkeit tun, indem er bei jeder bilateralen Kommunikation mit einem anderen Anwender AW2 dem Kommunikationspartner zunächst den öffentlichen Teil seines selbst generierten Schlüsselpaares ÖVS mit dem geheimen Teil des zuvor vom Trust Center überlassenen, personalisierten und zertifizierten Schlüsselpaares PS signiert und zustellt.

Der empfangende Kommunikationspartner AW2 kann die korrekte Zuordnung dieser Information hinsichtlich des öffentlichen Teils ÖVS des vom sendenden Anwenders AW1 selbst generierten Schlüsselpaares durch eine Verifikation der Signatur zuverlässig prüfen und gegebenenfalls die Echtheit und Gültigkeit des dieser Signatur zugrundeliegenden Zertifikates im Trust Center überprüfen.

Patentansprüche:

1. Verfahren zur Generierung asymmetrischer Kryptoschlüssel beim Anwender, bei dem Schlüssel an einer zentralen, besonders abgesicherten Stelle, (Trust Center), bzw. im Zusammenwirken mit gesicherter Übermittlung zwischen dem Anwender und diesem Trust Center, beim Anwender generiert, personalisiert und zertifiziert werden, dadurch gekennzeichnet, daß

a. dem Anwender zuerst vom Trust Center ein bereits generiertes, personalisiertes und zertifiziertes Signaturschlüsselpaar (PS; ÖS) und dazu Komponenten zur Erzeugung eines bzw. mehrerer Verschlüsselungsschlüsselpaare (GEK) zugestellt wird,

b. vom Anwender danach ein weiteres eigenes Verschlüsselungsschlüsselpaar mit einem öffentlichen (ÖVS) und einem geheimen Teil (PVS) erzeugt, und der öffentliche Teil (ÖVS)mit dem zugestellten geheimen Teil (PS) des Signaturschlüssels signiert und das Ergebnis zum Trust Center übermittelt wird,

c. vom Trust Center danach die zweifelsfreie Zuordnung zum Anwender mittels des zertifizierten öffentlichen Teils (ÖS) des Signaturschlüsselpaares geprüft wird,

d. vom Trust Center, nach erfolgreicher Zuordnungsprüfung, unter Verwendung von wenigstens einem öffentlichen Teil des Signaturschlüsselpaares (ÖS) bzw. des Verschlüsselungsschlüsselpaares (ÖVS) des Anwenders ein neues Zertifikat erzeugt wird, und zuletzt

e. vom Trust Center dieses Zertifikat, mit dem öffentlichen Teil des Verschlüsselungsschlüsselpaares (ÖVS) des Anwenders verschlüsselt, zum Anwender übermittelt wird.

2. Verfahren zur Generierung asymmetrischer Kryptoschlüssel beim Anwender nach Anspruch 1, dadurch gekennzeichnet, daß dem Anwender beim Verfahrensschritt a. zusätzlich Komponenten (GDSK) zur Erzeugung eines bzw. mehrerer Signaturschlüsselpaare zugestellt werden, welche beim Verfahrensschritt b. vom Anwender mit erzeugt werden, und daß vom Anwender auch der öffentliche Teil (ÖS2) dieses selbst generierten Signaturschlüsselpaares zugleich bzw. daneben mittels des geheimen Teils des vom Trust Center erhaltenen Signaturschlüsselpaares (PS) signiert wird.

3. Verfahren zur Generierung asymmetrischer Kryptoschlüssel beim Anwender nach Anspruch 1 und 2, dadurch gekennzeichnet, daß ein Anwender (AW1), der überhaupt keine Kommunikation mit einem Trust Center wünscht, bei jeder bilateralen Kommunikation mit einem anderen Anwender (AW2), diesem zunächst den öffentlichen Teil seines selbst generierten Schlüsselpaares (ÖVS bzw. ÖS2) mit dem geheimen Teil des zuvor vom Trust Center überlassenen, personalisierten und zertifizierten Schlüsselpaares (PS) signiert und zustellt, wonach vom empfangenden Anwender (AW2) die korrekte Zuordnung dieser Information hinsichtlich des öffentlichen Teils (ÖVS bzw. ÖS2) des vom sendenden Anwenders (AW1) selbst generierten Schlüsselpaares durch eine Verifikation der Signatur geprüft wird und die Echtheit und Gültigkeit des dieser Signatur zugrundeliegenden Zertifikates im Trust Center überprüft werden kann.

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT
AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts	**WEITERES VORGEHEN**	siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5
P96188WO.1P		
Internationales Aktenzeichen	Internationales Anmeldedatum *(Tag/Monat/Jahr)*	(Frühestes) Prioritätsdatum *(Tag/Monat/Jahr)*
PCT/EP 98/ 07984	09/12/1998	12/01/1998
Anmelder		
DEUTSCHE TELEKOM AG et al.		

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 3 Blätter.

[X] Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. **Grundlage des Berichts**

   a. Hinsichtlich der **Sprache** ist die internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.

   [ ] Die internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.

   b. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale Recherche auf der Grundlage des Sequenzprotokolls durchgeführt worden, das

   [ ] in der internationalen Anmeldung in Schriftlicher Form enthalten ist.

   [ ] zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.

   [ ] Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.

   [ ] Die Erklärung, daß die in computerlesbarer Form erfaßten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

2. [ ] **Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen** (siehe Feld I).

3. [ ] **Mangelnde Einheitlichkeit der Erfindung** (siehe Feld II).

4. Hinsichtlich der **Bezeichnung der Erfindung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut von der Behörde wie folgt festgesetzt:

5. Hinsichtlich der **Zusammenfassung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut nach Regel 38.2b) in der in Feld III angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der **Zeichnungen** ist mit der Zusammenfassung zu veröffentlichen: Abb. Nr. _____

   [ ] wie vom Anmelder vorgeschlagen [X] keine der Abb.

   [ ] weil der Anmelder selbst keine Abbildung vorgeschlagen hat.

   [ ] weil diese Abbildung die Erfindung besser kennzeichnet.

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 98/07984

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 H04L9/08 H04L9/32

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6 H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	WO 95 14283 A (HUGHES AIRCRAFT CO) 26. Mai 1995 siehe das ganze Dokument ---	1-3
A	US 5 606 617 A (BRANDS STEFANUS A) 25. Februar 1997 siehe Zusammenfassung siehe Spalte 3, Zeile 56 - Spalte 4, Zeile 34 siehe Spalte 5, Zeile 25 - Spalte 7, Zeile 59 siehe Anspruch 1 siehe Abbildung 1 --- -/--	1-3

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
27. April 1999	06/05/1999

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Gautier, L

1

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	US 5 513 245 A (MIZIKOVSKY SEMYON ET AL) 30. April 1996 siehe Zusammenfassung siehe Spalte 3, Zeile 45 - Spalte 4, Zeile 26 siehe Spalte 7, Zeile 16 - Zeile 41 siehe Anspruch 1 siehe Abbildung 5 -----	1,3

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP 98/07984

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
WO 9514283	A	26-05-1995	AU	669828 B	20-06-1996
			AU	8095794 A	06-06-1995
			CA	2149744 A,C	09-05-1995
			EP	0682832 A	22-11-1995
			JP	2723365 B	09-03-1998
			JP	8512445 T	24-12-1996
			NO	952584 A	27-06-1995
			US	5825300 A	20-10-1998
US 5606617	A	25-02-1997	AU	3755695 A	06-05-1996
			CA	2200592 A	25-04-1996
			EP	0786178 A	30-07-1997
			WO	9612362 A	25-04-1996
US 5513245	A	30-04-1996	US	5794139 A	11-08-1998

INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP 98/07984

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 : H04L9/08 H04L9/32
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 : H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

ES

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 95 14283 A (HUGHES AIRCRAFT CO) 26 May 1995 (26.05.95), See the whole document	1-3
A	US 5 606 617 A (BRANDS STEFANUS A) 25 February 1997 (25.02.97), See abstract See column 3, line 56 – column 4, line 34 See column 5, line 25 – column 7, line 59 See claim 1 See figure 1	1-3
A	US 5 513 245 A (MIZIKOVSKY SEMYON ET AL) 30 April 1996 (30.04.96), See abstract See column 3, Line 45 – Column 4, line 26 See Column 7, line 16 – line 41 See claim 1 See figure 5	1,3

☒ Further documents are listed in the continuation of box C. ☒ Patent family members are listed in annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot beconsidered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 April 1999 (27.04.99)	06 May 1999 (06.05.99)
Name and mailing address of the ISA/ European Patent Office	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP 98/07984

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9514283 A	26-05-1995	AU 669828 B	20-06-1996
		AU 8095794 A	06-06-1995
		CA 2149744 A,C	09-05-1995
		EP 0682832 A	22-11-1995
		JP 2723365 B	09-03-1998
		JP 8512445 T	24-12-1996
		NO 952584 A	27-06-1995
		US 5825300 A	20-10-1998
US 5606617 A	25-02-1997	AU 3755695 A	06-05-1996
		CA 2200592 A	25-04-1996
		EP 0786178 A	30-07-1997
		WO 9612362 A	25-04-1996
US 5513245 A	30-04-1996	US 5794139 A	11-08-1998

PCT

ANTRAG

Der Unterzeichnete beantragt, daß die vorliegende internationale Anmeldung nach dem Vertrag über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens behandelt wird.

Vom Anmeldeamt auszufüllen

Internationales Aktenzeichen: PCT/EP 98/07984

Internationales Anmeldedatum: 09 DEC 1998 (09. 12. 1998)

EUROPEAN PATENT OFFICE
PCT INTERNATIONAL APPLICATION
Name des Anmeldeamts und "PCT International Application"

Aktenzeichen des Anmelders oder Anwalts *(falls gewünscht)* *(max. 12 Zeichen)*: P96188WO.1P

Feld Nr. I BEZEICHNUNG DER ERFINDUNG

Verfahren zur Generierung asymetrischer Kryptoschlüssel beim Anwender

Feld Nr. II ANMELDER

Name und Anschrift: *(Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)*

DEUTSCHE TELEKOM AG
Friedrich-Ebert-Allee 140
D - 53113 Bonn
Deutschland

☐ Diese Person ist gleichzeitig Erfinder

Telefonnr.:

Telefaxnr.:

Fernschreibnr.:

Staatsangehörigkeit (Staat): DE

Sitz oder Wohnsitz (Staat): DE

Diese Person ist Anmelder für folgende Staaten: ☐ alle Bestimmungsstaaten ☒ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika ☐ nur die Vereinigten Staaten von Amerika ☐ die im Zusatzfeld angegebenen Staaten

Feld Nr. III WEITERE ANMELDER UND/ODER (WEITERE) ERFINDER

Name und Anschrift: *(Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)*

MERTES, Paul
Mertenseifer Grund 9
D- 57258 Freudenberg

Deutschland

Diese Person ist:

☐ nur Anmelder

☒ Anmelder und Erfinder

☐ nur Erfinder *(Wird dieses Kästchen angekreuzt, so sind die nachstehenden Angaben nicht nötig.)*

Staatsangehörigkeit (Staat): DE

Sitz oder Wohnsitz (Staat): DE

Diese Person ist Anmelder für folgende Staaten: ☐ alle Bestimmungsstaaten ☐ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika ☒ nur die Vereinigten Staaten von Amerika ☐ die im Zusatzfeld angegebenen Staaten

☒ Weitere Anmelder und/oder (weitere) Erfinder sind auf einem Fortsetzungsblatt angegeben.

Feld Nr. IV ANWALT ODER GEMEINSAMER VERTRETER: ZUSTELLANSCHRIFT

Die folgende Person wird hiermit bestellt/ist bestellt worden, um für den (die) Anmelder vor den zuständigen internationalen Behörden in folgender Eigenschaft zu handeln als: ☐ Anwalt ☒ gemeinsamer Vertreter

Name und Anschrift: *(Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben.)*

Deutsche Telekom AG.
Technologiezentrum, EK03

D - 64307 Darmstadt
Deutschland

Telefonnr.: +49 (61 51) 83-58 40

Telefaxnr.: +49 (61 51) 83-58 43

Fernschreibnr.:

☒ **Zustellanschrift:** Dieses Kästchen ist anzukreuzen, wenn kein Anwalt oder gemeinsamer Vertreter bestellt ist und statt dessen im obigen Feld eine spezielle Zustellanschrift angegeben ist.

EL179668701 US

Blatt Nr. 2

Fortsetzung von Feld Nr. III WEITERE ANMELDER UND/ODER (WEITERE) ERFINDER

Wird keines der folgenden Felder benutzt, so sollte dieses Blatt dem Antrag nicht beigefügt werden.

Name und Anschrift: *(Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)*

METTKEN, Werner
Eichenweg 9
D - 59969 Hallenberg

Deutschland

Diese Person ist:
- ☐ nur Anmelder
- ☒ Anmelder und Erfinder
- ☐ nur Erfinder *(Wird dieses Kästchen angekreuzt, so sind die nachstehenden Angaben nicht nötig.)*

Staatsangehörigkeit (Staat): DE

Sitz oder Wohnsitz (Staat): DE

Diese Person ist Anmelder für folgende Staaten: ☐ alle Bestimmungsstaaten ☐ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika ☒ nur die Vereinigten Staaten von Amerika ☐ die im Zusatzfeld angegebenen Staaten

Name und Anschrift: *(Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)*

Diese Person ist:
- ☐ nur Anmelder
- ☐ Anmelder und Erfinder
- ☐ nur Erfinder *(Wird dieses Kästchen angekreuzt, so sind die nachstehenden Angaben nicht nötig.)*

Staatsangehörigkeit (Staat):

Sitz oder Wohnsitz (Staat):

Diese Person ist Anmelder für folgende Staaten: ☐ alle Bestimmungsstaaten ☐ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika ☐ nur die Vereinigten Staaten von Amerika ☐ die im Zusatzfeld angegebenen Staaten

Name und Anschrift: *(Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)*

Diese Person ist:
- ☐ nur Anmelder
- ☐ Anmelder und Erfinder
- ☐ nur Erfinder *(Wird dieses Kästchen angekreuzt, so sind die nachstehenden Angaben nicht nötig.)*

Staatsangehörigkeit (Staat):

Sitz oder Wohnsitz (Staat):

Diese Person ist Anmelder für folgende Staaten: ☐ alle Bestimmungsstaaten ☐ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika ☐ nur die Vereinigten Staaten von Amerika ☐ die im Zusatzfeld angegebenen Staaten

Name und Anschrift: *(Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)*

Diese Person ist:
- ☐ nur Anmelder
- ☐ Anmelder und Erfinder
- ☐ nur Erfinder *(Wird dieses Kästchen angekreuzt, so sind die nachstehenden Angaben nicht nötig.)*

Staatsangehörigkeit (Staat):

Sitz oder Wohnsitz (Staat):

Diese Person ist Anmelder für folgende Staaten: ☐ alle Bestimmungsstaaten ☐ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika ☐ nur die Vereinigten Staaten von Amerika ☐ die im Zusatzfeld angegebenen Staaten

☐ Weitere Anmelder und/oder (weitere) Erfinder sind auf einem zusätzlichen Fortsetzungsblatt angegeben.

Feld Nr. V BESTIMMUNG VON STAATEN

Die folgenden Bestimmungen nach Regel 4.9 Absatz a werden hiermit vorgenommen *(bitte die entsprechenden Kästchen ankreuzen; wenigstens ein Kästchen muß angekreuzt werden)*:

Regionales Patent

- ☐ AP **ARIPO-Patent:** GH Ghana, GM Gambia, KE Kenia, LS Lesotho, MW Malawi, SD Sudan, SZ Swasiland, UG Uganda, ZW Simbabwe und jeder weitere Staat, der Vertragsstaat des Harare-Protokolls und des PCT ist
- ☐ EA **Eurasisches Patent:** AM Armenien, AZ Aserbaidschan, BY Belarus, KG Kirgisistan, KZ Kasachstan, MD Republik Moldau, RU Russische Föderation, TJ Tadschikistan, TM Turkmenistan und jeder weitere Staat, der Vertragsstaat des Eurasischen Patentübereinkommens und des PCT ist
- ☒ EP **Europäisches Patent:** AT Österreich, BE Belgien, CH und LI Schweiz und Liechtenstein, CY Zypern, DE Deutschland, DK Dänemark, ES Spanien, FI Finnland, FR Frankreich, GB Vereinigtes Königreich, GR Griechenland, IE Irland, IT Italien, LU Luxemburg, MC Monaco, NL Niederlande, PT Portugal, SE Schweden und jeder weitere Staat, der Vertragsstaat des Europäischen Patentübereinkommens und des PCT ist
- ☐ OA **OAPI-Patent:** BF Burkina Faso, BJ Benin, CF Zentralafrikanische Republik, CG Kongo, CI Côte d'Ivoire, CM Kamerun, GA Gabun, GN Guinea, ML Mali, MR Mauretanien, NE Niger, SN Senegal, TD Tschad, TG Togo und jeder weitere Staat, der Vertragsstaat der OAPI und des PCT ist *(falls eine andere Schutzrechtsart oder ein sonstiges Verfahren gewünscht wird, bitte auf der gepunkteten Linie angeben)* GW Guinea-Bissau

Nationales Patent *(falls eine andere Schutzrechtsart oder ein sonstiges Verfahren gewünscht wird, bitte auf der gepunkteten Linie angeben)*:

- ☐ AL Albanien
- ☐ AM Armenien
- ☐ AT Österreich
- ☐ AU Australien
- ☐ AZ Aserbaidschan
- ☐ BA Bosnien-Herzegowina
- ☐ BB Barbados
- ☐ BG Bulgarien
- ☐ BR Brasilien
- ☐ BY Belarus
- ☒ CA Kanada
- ☐ CH und LI Schweiz und Liechtenstein
- ☐ CN China
- ☐ CU Kuba
- ☐ CZ Tschechische Republik
- ☐ DE Deutschland
- ☐ DK Dänemark
- ☐ EE Estland
- ☐ ES Spanien
- ☐ FI Finnland
- ☐ GB Vereinigtes Königreich
- ☐ GE Georgien
- ☐ GH Ghana
- ☐ GM Gambia
- ☐ ~~GW Guinea-Bissau~~
- ☐ HR Kroatien
- ☐ HU Ungarn
- ☐ ID Indonesien
- ☐ IL Israel
- ☐ IS Island
- ☒ JP Japan
- ☐ KE Kenia
- ☐ KG Kirgisistan
- ☐ KP Demokratische Volksrepublik Korea
- ☐ KR Republik Korea
- ☐ KZ Kasachstan
- ☐ LC Saint Lucia
- ☐ LK Sri Lanka
- ☐ LR Liberia
- ☐ LS Lesotho
- ☐ LT Litauen
- ☐ LU Luxemburg
- ☐ LV Lettland
- ☐ MD Republik Moldau
- ☐ MG Madagaskar
- ☐ MK Die ehemalige jugoslawische Republik Mazedonien
- ☐ MN Mongolei
- ☐ MW Malawi
- ☐ MX Mexiko
- ☐ NO Norwegen
- ☐ NZ Neuseeland
- ☐ PL Polen
- ☐ PT Portugal
- ☐ RO Rumänien
- ☐ RU Russische Föderation
- ☐ SD Sudan
- ☐ SE Schweden
- ☐ SG Singapur
- ☐ SI Slowenien
- ☐ SK Slowakei
- ☐ SL Sierra Leone
- ☐ TJ Tadschikistan
- ☐ TM Turkmenistan
- ☐ TR Türkei
- ☐ TT Trinidad und Tobago
- ☐ UA Ukraine
- ☐ UG Uganda
- ☒ US Vereinigte Staaten von Amerika
- ☐ UZ Usbekistan
- ☐ VN Vietnam
- ☐ YU Jugoslawien
- ☐ ZW Simbabwe

Kästchen für die Bestimmung von Staaten (für die Zwecke eines nationalen Patents), die dem PCT nach der Veröffentlichung dieses Formblatts beigetreten sind:

- ☐ GD Grenada
- ☐ IN Indien

Erklärung bzgl. vorsorglicher Bestimmungen: Zusätzlich zu den oben genannten Bestimmungen nimmt der Anmelder nach Regel 4.9 Absatz b auch alle anderen nach dem PCT zulässigen Bestimmungen vor mit Ausnahme der im Zusatzfeld genannten Bestimmungen, die von dieser Erklärung ausgenommen sind. Der Anmelder erklärt, daß diese zusätzlichen Bestimmungen unter dem Vorbehalt einer Bestätigung stehen und jede zusätzliche Bestimmung, die vor Ablauf von 15 Monaten ab dem Prioritätsdatum nicht bestätigt wurde, nach Ablauf dieser Frist als vom Anmelder zurückgenommen gilt. *(Die Bestätigung einer Bestimmung erfolgt durch die Einreichung einer Mitteilung, in der diese Bestimmung angegeben wird, und die Zahlung der Bestimmungs- und der Bestätigungsgebühr. Die Bestätigung muß beim Anmeldeamt innerhalb der Frist von 15 Monaten eingehen.)*

Feld Nr. VI PRIORITÄTSANSPRUCH ☐ Weitere Prioritätsansprüche sind im Zusatzfeld angegeben.

Anmeldedatum der früheren Anmeldung (Tag/Monat/Jahr)	Aktenzeichen der früheren Anmeldung	Ist die frühere Anmeldung eine: nationale Anmeldung: Staat	regionale Anmeldung: * regionales Amt	internationale Anmeldung: Anmeldeamt
Zeile (1) 12.Januar1998 (12.01.1998)	198 01 241.1	DE		
Zeile (2)				
Zeile (3)				

☐ Das Anmeldeamt wird ersucht, eine beglaubigte Abschrift der oben in der (den) Zeile(n) _____ bezeichneten früheren Anmeldung(en) zu erstellen und dem internationalen Büro zu übermitteln *(nur falls die frühere Anmeldung(en) bei dem Amt eingereicht worden ist(sind), das für die Zwecke dieser internationalen Anmeldung Anmeldeamt ist)*

* *Falls es sich bei der früheren Anmeldung um eine ARIPO-Anmeldung handelt, so muß in dem Zusatzfeld mindestens ein Staat angegeben werden, der Mitgliedstaat der Pariser Verbandsübereinkunft zum Schutz des gewerblichen Eigentums ist und für den die frühere Anmeldung eingereicht wurde.*

Feld Nr. VII INTERNATIONALE RECHERCHENBEHÖRDE

Wahl der internationalen Recherchenbehörde (ISA) *(falls zwei oder mehr als zwei internationale Recherchenbehörden für die Ausführung der internationalen Recherche zuständig sind, geben Sie die von Ihnen gewählte Behörde an; der Zweibuchstaben-Code kann benutzt werden):*

ISA / EP

Antrag auf Nutzung der Ergebnisse einer früheren Recherche: Bezugnahme auf diese frühere Recherche *(falls eine frühere Recherche bei der internationalen Recherchenbehörde beantragt oder von ihr durchgeführt worden ist):*

Datum *(Tag/Monat/Jahr)* Aktenzeichen Staat *(oder regionales Amt)*

Feld Nr. VIII KONTROLLISTE; EINREICHUNGSSPRACHE

Diese internationale Anmeldung enthält die folgende **Anzahl von Blättern:**

Antrag	: 6
Beschreibung (ohne Sequenzprotokollteil)	: 4
Ansprüche	: 2
Zusammenfassung	: 1
Zeichnungen	: –
Sequenzprotokollteil der Beschreibung	: –
Blattzahl insgesamt	: 13

Dieser internationalen Anmeldung **liegen** die nachstehend angekreuzten Unterlagen **bei:**

1. ☒ Blatt für die Gebührenberechnung
2. ☐ Gesonderte unterzeichnete Vollmacht
3. ☒ Kopie der allgemeinen Vollmacht; Aktenzeichen (falls vorhanden): 34338
4. ☐ Begründung für das Fehlen einer Unterschrift
5. ☒ Prioritätsbeleg(e), in Feld Nr. VI durch folgende Zeilennummer gekennzeichnet:
6. ☐ Übersetzung der internationalen Anmeldung in die folgende Sprache:
7. ☐ Gesonderte Angaben zu hinterlegten Mikroorganismen oder anderem biologischen Material
8. ☐ Protokoll der Nucleotid- und/oder Aminosäuresequenzen in computerlesbarer Form
9. ☐ Sonstige *(einzeln aufführen)*:

Abbildung der Zeichnungen, die mit der Zusammenfassung veröffentlicht werden soll (Nr.):

Sprache, in der die internationale Anmeldung eingereicht wird: Deutsch

Feld Nr. IX UNTERSCHRIFT DES ANMELDERS ODER DES ANWALTS

Der Name jeder unterzeichnenden Person ist neben der Unterschrift zu wiederholen, und es ist anzugeben, sofern sich dies nicht eindeutig aus dem Antrag ergibt, in welcher Eigenschaft die Person unterzeichnet.

Deutsche Telekom AG

i.A. .....

Dr. Wilhelm Deuschel, Leiter Patentabteilung, EPA-Vollmacht Nr.34338

Erfinderunterschriften siehe Blatt 5 + 6

Vom Anmeldeamt auszufüllen

1. Datum des tatsächlichen Eingangs dieser internationalen Anmeldung: 09 DEC 1998 (-9. 12. 98)

2. Zeichnungen ☐ eingegangen: ☐ nicht eingegangen:

3. Geändertes Eingangsdatum aufgrund nachträglich, jedoch fristgerecht eingegangener Unterlagen oder Zeichnungen zur Vervollständigung dieser internationalen Anmeldung:

4. Datum des fristgerechten Eingangs der angeforderten Richtigstellungen nach Artikel 11(2) PCT:

5. Internationale Recherchenbehörde *(falls zwei oder mehr zuständig sind)*: ISA /

6. ☐ Übermittlung des Recherchenexemplars bis zur Zahlung der Recherchengebühr aufgeschoben

Vom Internationalen Büro auszufüllen

Datum des Eingangs des Aktenexemplars beim Internationalen Büro:

Zusatzfeld *Wird dieses Zusatzfeld nicht benutzt, so sollte dieses Blatt dem Antrag nicht beigefügt werden.*

1. Wenn der ***Platz in einem Feld nicht für alle Angaben ausreicht****: In diesem Fall schreiben Sie "Fortsetzung von Feld Nr. ..." [Nummer des Feldes angeben] und machen die Angaben entsprechend der in dem Feld, in dem der Platz nicht ausreicht, vorgeschriebenen Art und Weise, insbesondere:*

(i) ***Wenn mehr als zwei Anmelder und/oder Erfinder vorhanden sind*** *und kein "Fortsetzungsblatt" zur Verfügung steht: In diesem Fall schreiben Sie "Fortsetzung von Feld Nr. III" und machen für jede weitere Person die in Feld Nr. III vorgeschriebenen Angaben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.*

(ii) Wenn in Feld Nr. II oder III die Angabe ***"die im Zusatzfeld angegebenen Staaten"*** *angekreuzt ist: In diesem Fall schreiben Sie "Fortsetzung von Feld Nr. II", "Fortsetzung von Feld Nr. III" bzw. "Fortsetzung von Feld Nr. II und Nr. III" und geben den Namen des Anmelders oder die Namen der Anmelder an und neben jedem Namen den Staat oder die Staaten (und/oder ggf. ARIPO-, eurasisches, europäisches oder OAPI-Patent), für die die bezeichnete Person Anmelder ist.*

(iii) Wenn der in Feld Nr. II oder III genannte ***Erfinder oder Erfinder/Anmelder nicht für alle Bestimmungsstaaten oder für die Vereinigten Staaten von Amerika als Erfinder benannt ist****: In diesem Fall schreiben Sie "Fortsetzung von Feld Nr. II", "Fortsetzung von Feld Nr. III" bzw. "Fortsetzung von Feld Nr. II und Nr. III" und geben den Namen des Erfinders oder die Namen der Erfinder an und neben jedem Namen den Staat oder die Staaten (und/oder ggf. ARIPO-, eurasisches, europäisches oder OAPI-Patent), für die die bezeichnete Person Erfinder ist.*

(iv) Wenn zusätzlich zu dem Anwalt oder den Anwälten, die in Feld Nr. IV angegeben sind, ***weitere Anwälte*** *bestellt sind: In diesem Fall schreiben Sie "Fortsetzung von Feld Nr. IV" und machen für jeden weiteren Anwalt die entsprechenden, in Feld Nr. IV vorgeschriebenen Angaben.*

(v) Wenn in Feld Nr. V bei einem Staat (oder bei OAPI) die Angabe ***"Zusatzpatent"*** *oder* ***"Zusatzzertifikat."*** *oder wenn in Feld Nr. V bei den Vereinigten Staaten von Amerika die Angabe* ***"Fortsetzung"*** *oder* ***"Teilfortsetzung"*** *hinzugefügt wird: In diesem Fall schreiben Sie "Fortsetzung von Feld Nr. V" und geben den Namen des betreffenden Staats (oder OAPI) an und nach dem Namen jedes solchen Staats (oder OAPI) das Aktenzeichen des Hauptschutzrechts oder der Hauptschutzrechtsanmeldung und das Datum der Erteilung des Hauptschutzrechts oder der Einreichung der Hauptschutzrechtsanmeldung.*

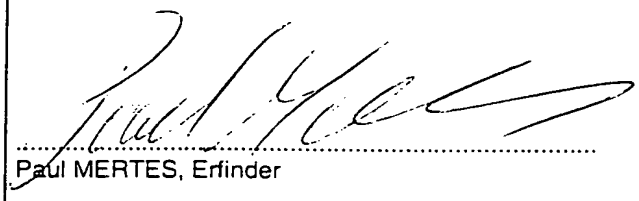
(vi) Wenn in Feld Nr. VI ***die Priorität von mehr als drei früheren Anmeldungen beansprucht wird****: In diesem Fall schreiben Sie "Fortsetzung von Feld Nr. VI" und machen für jede weitere frühere Anmeldung die entsprechenden, in Feld Nr. VI vorgeschriebenen Angaben.*

(vii) Wenn in Feld Nr. VI die ***frühere Anmeldung eine ARIPO Anmeldung*** *ist: In diesem Fall schreiben Sie "Fortsetzung von Feld Nr. VI" und geben, unter Angabe der Nummer der Zeile, in der die die frühere Anmeldung betreffenden Angaben gemacht sind, mindestens einen Staat an, der Mitglied der Pariser Verbandsübereinkunft zum Schutz des gewerblichen Eigentums ist und für den die frühere Anmeldung erfolgte.*

2. Wenn, im Hinblick auf die ***Erklärung bzgl. vorsorglicher Bestimmungen*** *in Feld Nr. V, der Anmelder Staaten von dieser Erklärung ausnehmen möchte: In diesem Fall schreiben Sie "Bestimmung(en), die von der Erklärung bzgl. vorsorglicher Bestimmungen ausgenommen ist(sind)" und geben den Namen oder den Zweibuchstaben-Code jedes so ausgeschlossenen Staates an.*

3. Wenn der Anmelder für irgendein Bestimmungsamt die Vorteile nationaler Vorschriften betreffend ***unschädliche Offenbarung oder Ausnahmen von der Neuheitsschädlichkeit*** *in Anspruch nimmt: In diesem Fall schreiben Sie "Erklärung betreffend unschädliche Offenbarung oder Ausnahmen von der Neuheitsschädlichkeit" und geben im folgenden die entsprechende Erklärung ab.*

Fortsetzungvon Feld IX (Unterschrift des Anmelders)



Paul MERTES, Erfinder

Zusatzfeld *Wird dieses Zusatzfeld nicht benutzt, so sollte dieses Blatt dem Antrag nicht beigefügt werden.*

*1. Wenn der **Platz in einem Feld nicht für alle Angaben ausreicht**: In diesem Fall schreiben Sie "Fortsetzung von Feld Nr. ..." [Nummer des Feldes angeben] und machen die Angaben entsprechend der in dem Feld, in dem der Platz nicht ausreicht, vorgeschriebenen Art und Weise, insbesondere:*

*(i) **Wenn mehr als zwei Anmelder und/oder Erfinder vorhanden sind** und kein "Fortsetzungsblatt" zur Verfügung steht: In diesem Fall schreiben Sie "Fortsetzung von Feld Nr. III" und machen für jede weitere Person die in Feld Nr. III vorgeschriebenen Angaben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.*

*(ii) Wenn in Feld Nr. II oder III die Angabe **"die im Zusatzfeld angegebenen Staaten"** angekreuzt ist: In diesem Fall schreiben Sie "Fortsetzung von Feld Nr. II", "Fortsetzung von Feld Nr. III" bzw. "Fortsetzung von Feld Nr. II und Nr. III" und geben den Namen des Anmelders oder die Namen der Anmelder an und neben jedem Namen den Staat oder die Staaten (und/oder ggf. ARIPO-, eurasisches, europäisches oder OAPI-Patent), für die die bezeichnete Person Anmelder ist.*

*(iii) Wenn der in Feld Nr. II oder III genannte **Erfinder oder Erfinder/Anmelder nicht für alle Bestimmungsstaaten oder für die Vereinigten Staaten von Amerika als Erfinder benannt ist**: In diesem Fall schreiben Sie "Fortsetzung von Feld Nr. II", "Fortsetzung von Feld Nr. III" bzw. "Fortsetzung von Feld Nr. II und Nr. III" und geben den Namen des Erfinders oder die Namen der Erfinder an und neben jedem Namen den Staat oder die Staaten (und/oder ggf. ARIPO-, eurasisches, europäisches oder OAPI-Patent), für die die bezeichnete Person Erfinder ist.*

*(iv) Wenn zusätzlich zu dem Anwalt oder den Anwälten, die in Feld Nr. IV angegeben sind, **weitere Anwälte** bestellt sind: In diesem Fall schreiben Sie "Fortsetzung von Feld Nr. IV" und machen für jeden weiteren Anwalt die entsprechenden, in Feld Nr. IV vorgeschriebenen Angaben.*

*(v) Wenn in Feld Nr. V bei einem Staat (oder bei OAPI) die Angabe **"Zusatzpatent"** oder **"Zusatzzertifikat,"** oder wenn in Feld Nr. V bei den Vereinigten Staaten von Amerika die Angabe **"Fortsetzung"** oder **"Teilfortsetzung"** hinzugefügt wird: In diesem Fall schreiben Sie "Fortsetzung von Feld Nr. V" und geben den Namen des betreffenden Staats (oder OAPI) an und nach dem Namen jedes solchen Staats (oder OAPI) das Aktenzeichen des Hauptschutzrechts oder der Hauptschutzrechtsanmeldung und das Datum der Erteilung des Hauptschutzrechts oder der Einreichung der Hauptschutzrechtsanmeldung.*

*(vi) Wenn in Feld Nr. VI **die Priorität von mehr als drei früheren Anmeldungen beansprucht wird**: In diesem Fall schreiben Sie "Fortsetzung von Feld Nr. VI" und machen für jede weitere frühere Anmeldung die entsprechenden, in Feld Nr. VI vorgeschriebenen Angaben.*

*(vii) Wenn in Feld Nr. VI die **frühere Anmeldung eine ARIPO Anmeldung** ist: In diesem Fall schreiben Sie "Fortsetzung von Feld Nr. VI" und geben, unter Angabe der Nummer der Zeile, in der die die frühere Anmeldung betreffenden Angaben gemacht sind, mindestens einen Staat an, der Mitglied der Pariser Verbandsübereinkunft zum Schutz des gewerblichen Eigentums ist und für den die frühere Anmeldung erfolgte.*

*2. Wenn, im Hinblick auf die **Erklärung bzgl. vorsorglicher Bestimmungen** in Feld Nr. V, der Anmelder Staaten von dieser Erklärung ausnehmen möchte: In diesem Fall schreiben Sie "Bestimmung(en), die von der Erklärung bzgl. vorsorglicher Bestimmungen ausgenommen ist(sind)" und geben den Namen oder den Zweibuchstaben-Code jedes so ausgeschlossenen Staates an.*

*3. Wenn der Anmelder für irgendein Bestimmungsamt die Vorteile nationaler Vorschriften betreffend **unschädliche Offenbarung oder Ausnahmen von der Neuheitsschädlichkeit** in Anspruch nimmt: In diesem Fall schreiben Sie "Erklärung betreffend unschädliche Offenbarung oder Ausnahmen von der Neuheitsschädlichkeit" und geben im folgenden die entsprechende Erklärung ab.*

Fortsetzungvon Feld IX (Unterschrift des Anmelders)

W. Mettken

.....

Werner METTKEN, Erfinder